AD-A076 620 HAWAII UNIV HONOLULU F/G 17/2
MILITARY DATA NETWORKS: PRESENT PLANS AND FUTURE REQUIREMENTS,(U)
1979 F KUO , I LEBOW , R LYONS , C WILCOX N00014-78-C-0498

UNCLASSIFIED NL

| OF |

AD
A076620

END
DATE
FILMED
12-79
DDC

(12)

LEVEL II

Panel Paper (11) 1979

(6)

MILITARY DATA NETWORKS: PRESENT PLANS AND FUTURE REQUIREMENTS

(12) 7

(10)
Moderator: Franklin Kuo, University of Hawaii* (Dept Elec. Eng) Honolulu
Panelists: Irwin Lebow, Defense Communications Agency
Robert Lyons, Defense Communications Agency
Chris Wilcox, Office of the Secretary of Defense
Thomas Bartee, Institute for Defense Analyses

To appear in the Proceedings of the Sixth Data Communications Symposium November 27-29, 1979, Pacific Grove, California. Published by the IEEE Computer Society

(15) N00014-78-C-0498

*The effort of organizing and coordinating the material in the panel was supported by the Office of Naval Research under Contract N00014-78-C-0498

ABSTRACT

Contents: Introductory remarks; Secure voice systems and technology; AUTODIN, the DoD Common-User Communications Network; Automated message handling systems; Standards for DoD Network applications.

/

PANEL ON MILITARY DATA NETWORKS: PRESENT PLANS AND FUTURE REQUIREMENTS

Moderator: Franklin F. Kuo, University of Hawaii
Panelists: Irwin Lebow, Defense Communications Agency
Robert E. Lyons, Defense Communications Agency
Chris N. Wilcox, Office of the Secretary of Defense
Thomas Bartee, Institute for Defense Analysis

Moderator's Remarks
Introduction to the Panel

The Defense Communications System (DCS) provides the basic US defense communications capabilities for peacetime as well as wartime applications. Two of the major systems in the DCS are the secure voice communications net, AUTOSEVOCOM (Automatic Secure Voice Network) and the secure data and message transmission net, AUTODIN I (Automatic Digital Network I). At present there are a number of ongoing defense programs to improve and modernize the DCS. In this session we will discuss a number of these programs. The papers to be presented are:
Secure Voice Programs and Technology, presented by Irwin L. Lebow, the Chief Scientist of the Defense Communications Agency (DCA).
AUTODIN: The DoD Common-User Data Communications Network, given by Robert E. Lyons, of the Defense Communications Engineering Center of DCA.
Automated Message Handling Systems, presented by Chris N. Wilcox of the Information Systems Directorate of the Office of the Assistant Secretary of Defense, (Communications, Command, Control and Intelligence).
Standards for DoD Network Applications, by Thomas Bartee of the Institute for Defense Analysis (IDA) and Harvard University.

In the first talk, Dr. Lebow will discuss DoD plans for providing secure voice for three disparate communities within DoD: 1. Narrowband Tactical (datarate: up to 2.4 KB), 2. Wideband Tactical (16 and 32 KB) and 3. Long-haul Strategic (DCS-based, up to 9.6 KB). Dr. Lebow will compare advantages and deficiencies of the three systems and will discuss the evolution of these systems into a two-rate architecture in the 1990's.

In the second paper, Dr. Lyons will discuss the DoD system architecture concept for the evolutionary growth of defense data networks: the Integrated AUTODIN System Architecture (IASA).

The third paper, presented by Lt. Col. Wilcox will discuss DoD plans for the integrated development of standard Automated Message Handling (AMH) systems for military end-user applications.

The final paper, by Dr. Bartee, is a discussion of protocol standardization requirements for the interconnection of present and future DoD data networks such ARPANET, AUTODIN I & II, and other DoD data handling networks such as Intelligence community's COINS II (Community On-line Intelligence Network System), and IDHSC II (Intelligence Data Handling System Communications). Bartee will conclude his talk with a discussion of database management problems in computer networks. The discussion will emphasize the data acquisition problem.

The session will conclude with a panel discussion among the authors, with questions from the session chairman and the audience.

Irwin Lebow's Remarks
Secure Voice Systems and Technology

Secure voice service is provided by digitizing and then encrypting the speech at the source, transmitting the encrypted digits over the communications medium and then converting the received digits to speech. The essential technical problem is that of achieving "acceptable" speech quality at an "acceptable" system cost with terminal equipment (voice processors, cryptos and modems) meeting environmental constraints appropriate to the user. The voice processing can be performed using a variety of techniques at digitization rates varying from below 2.4 to above 50 Kbits/sec. In general the higher the rate the higher the transmission costs but, the better the resultant speech quality and the lower the voice processing costs.

Today's technology limitations render it difficult to provide secure voice economically even for a relatively homogeneous community of subscribers. Providing secure voice for several disparate communities so as to permit interoperability among them all is of the highest importance to the Defense Department but is a still harder problem.

There are three such secure voice communities in the DoD:

1. "Narrowband tactical," a set of users mostly but not exclusively in the Navy limited to communications channels such as HF radio and UHF satellite which can support at most a rate of 2.4 Kbits/sec.
2. "Wide-band tactical," a set of tactical users mostly highly mobile ground forces for whom almost any data rate is acceptable but whose voice terminals must be lightweight and consume low power.
3. "Long-haul strategic," or the Defense Communications System (DCS) constrained to use AUTOVON, the currently analog plant providing clear voice service for the DoD. The data rate must be supportable over 4 kHz voice-frequency channels and the quality must be good enough to be comparable to the telephone. Interoperability with the other two communities is of prime importance.

Secure voice systems are being developed for

each of these communities to be fielded within the next few years. The "narrow-band tactical" community will use a terminal called the Advanced Narrow-band Digital Voice Terminal (ANDVT) incorporating a linear-predictive coding speech processor at a rate of 2.4 Kbits/sec. It produces intelligible but somewhat artificial speech. The "wideband tactical community" will use a terminal called the Digital Secure Voice Terminal (DSVT) incorporating a continuously variable slope delta modulation (CVSD) processor at 16 and 32 Kbits/sec. Its quality is quite good at the high rate, good but somewhat degraded at the low rate. The DCS secure voice component will use a terminal similar to one under development for civil use. Its primary rate will be 9.6 Kbits/sec using adaptive predictive coding (APC). A back-up rate of 2.4 Kbits/sec uses a processor identical to that in the ANDVT. Telephone line modems at both rates are included in the terminal. In addition, a 16 Kbits/sec CVSD voice processor is provided. Thus this terminal with an external modem is directly interoperable with the DSVT. The 9.6 Kbits/sec system achieves a fairly good quality different than but roughly equivalent to 16 Kbits/sec CVSD.

This 4-rate secure voice architecture should evolve to a two rate architecture in the 1990's. Technology should permit the development of a 16 Kbits/sec system comparable in quality to 32 Kbits/sec CVSD in a package suitable for the "wide-band tactical" environment. Further, in that time frame the analog telephone plant should be mostly digitized permitting this new high-quality 16 Kbits/sec system to be the primary DCS mode. This development should thus permit the phase-out of the 32 and 9.6 Kbits/sec rates. The 2.4 Kbits/sec rate will remain as the most survivable element of the architecture through its ability to be supported by almost all communications media even under degraded conditions.

While unexpected technology advances could bring the hi-quality rate down below 16 Kbits/sec perhaps as low as 9.6 Kbits/sec, it is unlikely that 2.4 Kbits/sec will achieve high enough quality to serve as a universal rate.

Robert Lyon's Remarks
AUTODIN: The Department of Defense Common-User Data Communications Network

1. Introduction. "AUTODIN" is the name originally applied to the "Automated Digital Network", a store-and-forward message service offering for Department of Defense users, since the early 1960's. Today, that earlier service is known as "AUTODIN I", and the term "AUTODIN" is applied to a total integrated data communications network which serves all common-user data communications needs of the Defense Department. The Integrated AUTODIN System Architecture is a prescription for growth of this AUTODIN network considering it as providing a total end-to-end data communications service. The Integrated AUTODIN System includes not only AUTODIN I, but also AUTODIN II, DoD's new packet-switched network, and other elements such as a standard terminal family and gateways to other networks.

2. AUTODIN II -- The IAS Backbone. The AUTODIN II network has been identified as the common-user backbone communications system which will serve as the basic interconnection mechanism for all of the other elements of the Integrated AUTODIN System (IAS). The following attributes are fundamental to AUTODIN II in this role: (1) it is a computer communication system, and the other elements of the IAS are, in fact, computers or computer terminals; (2) it has the security features required of a military system; (3) it is an ultra-reliable data transport mechanism; (4) it is planned to grow to world-wide dimensions, such that connections to multiple nodes will be generally available everywhere, as a survivability feature; (5) it provides for a variety of connection methods, including gateways to other networks for interoperability.

3. The Many Kinds of AUTODIN II Hosts. The basic backbone of AUTODIN II is a mesh of packet-switched nodes called "Switch Control Modules" (SCM's) which are functionally analogous to ARPANET IMP's (Interface Message Processors). Hosts are connected to the SCM's via a Segment Interface Protocol (SIP), and must have the standard Transmission Control Protocol (TCP) to pass useful traffic to other hosts. There are several kinds of hosts:

(a) A Terminal Access Controller (TAC) is a special host provided by the network itself to serve those users who wish to connect terminals directly to the network. The TAC is the analog of the terminal access portion of an ARPANET TIP (Terminal Interface Processor). It provides standard SIP/TCP protocols, plus the AUTODIN II standard Terminal-to-Host Protocol (THP). TAC's are generally colocated with SCM's to form a total AUTODIN II node, but there are plans for providing remote TAC's within AUTODIN II.

(b) Another special host of the IAS is the AUTODIN Switching Center (ASC). This is the present-day AUTODIN I switch, which continues to serve as a host to a disc storage system which stores and forwards the formal DoD message traffic. A special protocol will be used among ASC's so that they can exchange message traffic among themselves, as a community of interest, just as they do today over dedicated lines to perform the AUTODIN I functions.

(c) Another special type of host of the IAS is the Message Processing Computer (MPC), including the Automated Message Processing Exchange (AMPE). AMPE's are sophisticated AUTODIN terminals which automate many of the functions of a telecommunications center (message file, retrieval, distribution, etc.). Today's AMPE's are connected to ASC's directly, but our model for the future IAS has them connected to the AUTODIN II backbone, just like any other computer host. They will continue to reach ASC's via the AUTODIN II backbone initially, but later, as obsolete ASC hardware is phased out, AMPE's will obtain message services via a special Virtual

Message Protocol. Other MPC's include the NATO TARE (Teletype Automatic Routing Exchange) and the AN/TYC-39 tactical message switch. Initially these systems will continue to be connected to ASC's, but as the ASC hardware is phased out and AUTODIN II switches become ubiquitous, they too can become AUTODIN II hosts sharing in the Virtual Message Protocol. Alternatively, TARE networks and tactical message networks can be connected via the gateway mechanisms described below.

(d) Users who wish to take advantage of the availability of a reliable, secure, survivable packet-switched backbone can join the network en masse as an AUTODIN II subnetwork. Thus the WIN (WWMCCS Intercomputer Network) and the SACDIN (SAC Digital Network) are examples of AUTODIN II subnetworks, and their computers will join the network as special hosts. They will use the AUTODIN II standard SIP and will also be required to use the DoD standard TCP unless they can obtain a waiver from this requirement based on the lack of need to communicate with others beyond their own subnet community of interest. (A DoD initiative to encourage interoperability among subnets by adopting required standard host-to-host protocols will be treated in a companion paper.)

(e) Other computers requiring communications to remote terminals or hosts for any authorized purpose whatever will, of course, be able to join the network as general service subscribers. To decrease the burden on host computers to add special networking software, the AUTODIN II design provides a variety of access methods. For example, a single channel control unit (SCCU) or multi-channel control unit (MCCU) is provided by the contractor and the SIP/TCP software is included in these units, removing the user's burden of providing that software in his host. Instead, he need only provide relatively simple software to meet a Host Specific Interface in the CCU which would be provided by the AUTODIN II system. Optionally, the user can provide his own SIP/TCP software in his host or in a special front-end processor, so long as this software conforms to the standard specification required of AUTODIN II subscribers.

4. Gateways and internetting. One final AUTODIN II interface remains to be described, and that is an interface not to a host, but to another network via a gateway. Although most DoD computer communications users are required to subscribe to AUTODIN II either as general service subscribers or private subnetworks, there remain a few highly specialized networking applications which may justify separate networks. Certain intelligence community applications are in this category, for example. DoD policy requires, as a minimum, that such special-purpose networks at least be capable of interfacing to AUTODIN II via gateways to provide for interoperability, restoral of connectivity in crisis situations, and the like. Moreover, gateways can provide temporary or permanent connectivity among AUTODIN II subscribers and subscribers of such diverse networks as ARPANET, future tactical packet radio networks, and tactical and allied military message communication networks. To achieve this desired interoperability, it is required that the subscribers of internetted systems use a common standard TCP and Internet Protocol (IP). DoD policy has recently been stated which requires DoD data network subscribers having requirements for interoperability to adhere to these standards. What remains is for the gateways themselves to be developed and implemented.

Chris Wilcox's Remarks
Automated Message Handling Systems

There are in excess of 30 systems in operation or advanced stages of development in DoD that provide services categorized as automated message handling. They serve a broad spect um of commands and message handling needs.

In addition to the automation of switching centers and communications centers undertaken in the 1960's and 1970's, we are now addressing the large volume of message traffic flowing into major command and intelligence watch centers with the objective of improving internal distribution, review, filing, retrieval and composition. Whereas the first two stages automated the tasks of communications personnel, the third stage applies automation to the needs of originators and recipients. The primary utility of the third stage, or user oriented systems, is in increasing the ability of action officers to deal effectively with the high volumes of traffic encountered in crisis situations. The volumes of message traffic under stressed conditions, the vital importance of timely message review and action, the potentially serious consequences of error, and the availability of state-of-the-art technology drive us toward automated solutions for command/watch center problems.

The potential benefits, given today's technology, go far beyond message handling efficiencies. This kind of system can be a viable substitute for formatted file reporting systems that are causing problems in terms of acuracy, timeliness, and consistency across command boundaries--especially in fast moving crisis situations where our formatted systems and WWMCCS ADP in general are not providing the desired level of support. Message handling automation can channel information quickly to interested staff officers and with even a limited data base management system can facilitate the decision process.

In January 1979, the Department of Defense published a comprehensive plan for improving the management and continuing the evaluation of AMH systems. Under the DoD AMH Plan, the Defense Communications Agency has been given central architectural management responsibility to include those functions necessary to achieve and maintain more effective levels of interoperability, commonality and standardization across the spectrum of DoD AMH

systems.

The plan sets policy guidelines regarding the evolution and development of AMH systems. Whenever possible service and agency user-oriented and communications center message handling requirements will be satisfied through standard systems.

Thomas Bartee's Remarks
Standards for DoD Network Applications

The DoD is a major developer of computer networks. These networks have been independently developed by different parts of DoD in response to differing requirements. As a result, and because of the newness of the technology, these networks differ in a number of technical characteristics.

A need has been perceived to interconnect these networks and this need, along with the drive to develop a communications system (AUTODIN II) for widespread data transmission in the DoD has led to a program to develop the standards necessary for internetworking. Other advantages include the economic, operational, and developmental advantages which accrue from standards adoption.

In order to interconnect two or more computer networks successfully, using communications links, certain procedures and rules of operation must be adhered to. The first section of this presentation will concentrate on standards development for the protocols necessary to successful computer internetting. Most of the considerations for DoD networks are similar to those for commercial usage except some features are more heavily emphasized in DoD systems (security and precedence are notable examples). Further, our considerations also include the gateways needed to interconnect existing and new networks and a discussion of desirable gateway properties, including simplicity and "hot switchover" will be given. Dynamic rerouting in general will also be discussed as will other desirable properties for DoD systems.

In order to develop the necessary underlying technology for DoD systems, DARPA has been an active sponsor of computer network R&D and the ARPANET is a notable example of a packet switched computer network which is a test vehicle for DoD system development.

Figure 1 shows the protocol layout for ARPANET which will provide a background for discussion.

Figure 2 shows a block diagram of a possible layout for future DoD usage. Included are voice, conferencing, and other new protocols which seem desirable for DoD usage. A discussion of this layout and the reasons for some of the features will be presented.

The second section of the presentation will discuss data base management in computer networks. When computer networks already containing a number of data bases and differing data base management systems are interconnected, certain already existing problems are further emphasized. For example, the query languages for the data bases will generally differ, and so users are presented with a new version of the "Tower of Babel" which they must contend with in order to access data. Further, the differing structures of the files in the various systems must be considered and even the names of the desired data items may differ and must somehow be arrived at.

The discussion will emphasize the data acquisition problem and not that for updating files at remote locations. The various schemes which have been proposed to alleviate this problem will be presented along with some analysis of their desirability.

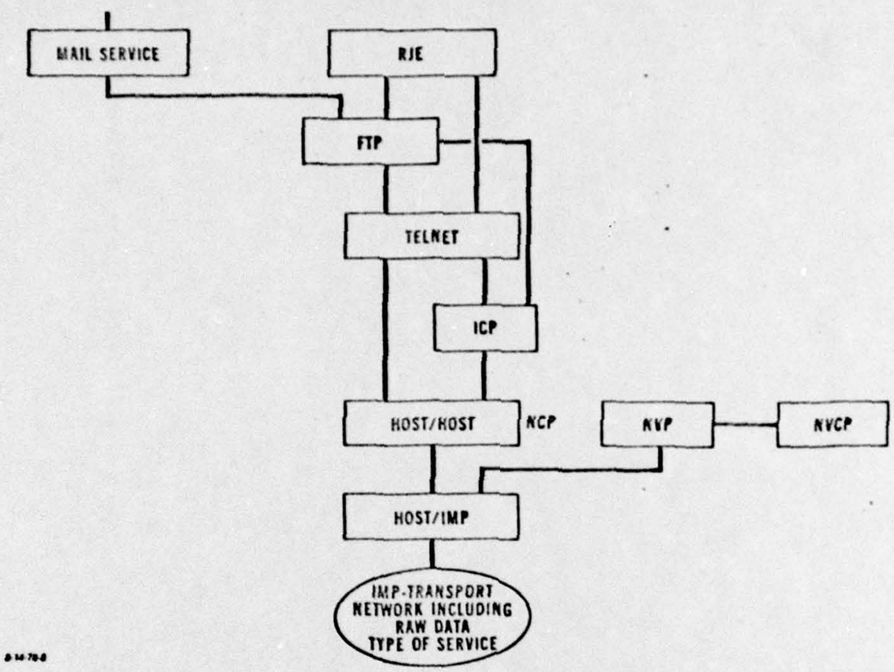

FIGURE 1. ARPANET Protocols

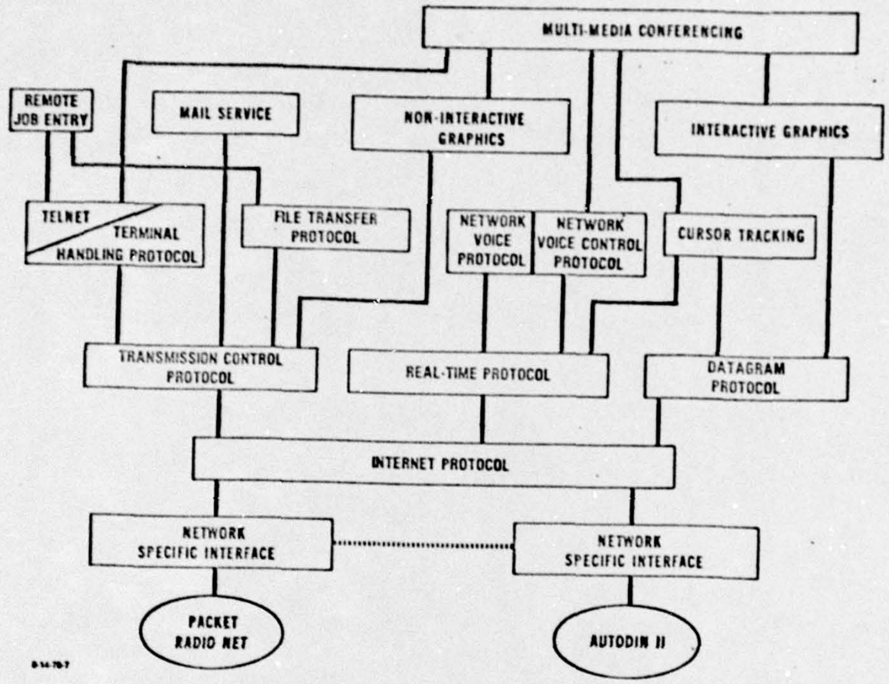

FIGURE 2. Protocol Architecture